A Secure Connection: Finding the Form of ASEAN Cyber Security Cooperation

Krisman, Khanisa

Veröffentlichungsversion / Published Version
Zeitschriftenartikel / journal article

Empfohlene Zitierung / Suggested Citation:
Krisman, K. (2013). A Secure Connection: Finding the Form of ASEAN Cyber Security Cooperation. *Journal of ASEAN Studies*, *1*(1), 41-53. https://nbn-resolving.org/urn:nbn:de:0168-ssoar-441755

A Secure Connection: Finding the Form of ASEAN Cyber Security Cooperation

Khanisa *Centre for Political Studies, Indonesia Institute of Sciences (LIPI)*

Abstract

Internet security is somehow being understated in ASEAN's strategy facing 2015. ASEAN Connectivity as the blue print of ASEAN's development strategy to strengthen the regional bond has not put proper attention in building security for guiding the connectivity plan among ASEAN member countries. This paper will discuss the future of cyber security cooperation particularly as ASEAN is planning to connect the region through ICT. This paper will try to analyse what kind of framework ASEAN will need on preparation to widen its security agenda to cyber world in the future to complete its preparation of being connected.

Keywords: Internet Security, Cooperation, ASEAN

Introduction

As the wave of technology and modernity changes the way of our daily life, it has changed the world's perception some of its values as well. One of the icons of this technological development is the internet which at first serves as the communication network in the cold war (Ryan, 2010, p. 14). The internet nowadays also has created a new realm, cyberspace, and in the era of high-speed connection, many people labelled the cyberspace as a lawless and borderless world of which freedom is the main issue. Anyone supposed to be free to be connected, search for anything they need from every source they find and transform their creation in digital form. Some people even go beyond and use the internet to get what they need in illegal ways. This can be a general description of what will be later categorized as cybercrime.

Although there are still many discussions about the interpretation of cyber-crime due to its vast scope of infringement, it is important to have a basic understanding about what cybercrime really is. Using computer as a tool to commit a crime is not necessarily called a cybercrime. There is a difference of cybercrime and computer crime. Cybercrime is not only a crime committed with digital instrument, but it also connected to the network of digital communication (Gerkce, 2011, p. 26). The connectivity issue makes cybercrime more complex to deal with. As a measure to avert the future damage caused by cybercrime, laws and regulations governing the cyberspace are created to prevent them to

Journal of ASEAN Studies, Vol.1,No.1 (2013), pp. 41–53

ISSN 2338-1361 print / ISSN2338-1353 electronic

happen. Some of the first emerged in the 1990s, like Britain's Computer Misuse Act (1990), Ireland's The Criminal Damage Act (1991), Malaysia's Computer Crimes Act (1997) (Singh, 2007, p. 79) and until now the growth of such laws and legislations continues as cybercrime expands. But the volume of cybercrime threats also goes parallel with the counter measures formulated by the government. Nevertheless, cybercrime developed and extended its complexity and the actors also getting well-organized.

The international community has acknowledged that this new threat can be global level security issues as many of the high scale businesses and administrations are run on digitalized systems which are fragile enough to be ruined by viruses created by hackers. Due to that reason, the internet nowadays is treated more than a communication channel; as it has now included on a country "territorial" space. The awareness to treat cyber security more seriously can be seen as some countries started to build cyber security cooperation. The first convention arranging such cooperation is the 2001 Convention on Cybercrime held in Budapest by the Council of Europe; with 39 countries have ratified the convention (Council of Europe Treaty Office, 2013).

Unfortunately, an arrangement like the Council of Europe's Convention on Cybercrime is commonly preferred by democratic and developed countries. For developing region especially in Southeast Asia, this kind of cooperation will have to wait to be prioritized. In Southeast Asia, some of the countries may have developed in cyber technology and at the same time have cybercrime prevention unit. Others may have not gone that far. Countries in Southeast Asia seem to be unprepared to design cyber security cooperation as a consequence of gaps in development of Information and Communications Technology (ICT).

Despite these gaps and differences, ASEAN has planned three regional blueprints; in one of them is in the political-security field which includes the ASEAN Regional Forum, an establishment to promote peace and security in the wider East-Asia region which also deals with the unconventional security issue like cybercrime. ASEAN also put ICT development as integral part of the ASEAN Connectivity. The development of ICT should not only address on strengthening of the network but also the prevention from threats or attacks on that network. Like many ASEAN cooperation, ASEAN have to struggle to synchronize the point of view of its members on the importance of such cooperation. Since each member countries is in different phase of their ICT development and their dealings with cybercrime.

In this paper, the author argues that ASEAN have to be prepared for dynamic changes in the security field which makes cyber domain as one of its source of new threat and regional security framework has to be designed to cope with such issue as it is a transnational type of disturbance that inter-state cooperation is nedeed. Based on that argument, this paper firstly will discuss about the aspect of the growth of ICT in the region of Southeast Asia to know how far ICT impacting ASEAN member states, and the later part of this paper will assess how ASEAN, as a regional organization, build its cyber security agenda. The question is "what kind of cyber security cooperation should be implemented in region?"

For answering the question, the author examines several formal documents such as Convention of Cybercrime, NATO's Policy on cyber defence, APCERT framework and also ASEAN's Charter and documentation from ASEAN's meetings and forums. This approach is substantial to know whether

the existed framework will be suitable to be taken building foundation for ASEAN's future cyber security cooperation. Some reports and news also used to recognize the current trends and situation in the issue of cyber security and cybercrime.

Although not specifically discuss theoretical topic of security in later segments, this paper is built on the author perspective of dynamic changes in International Relations especially in the field of security. In the author's opinion, the need of cyber security is caused by the enlargement domain of dwelling and interaction of the internet user which as not only consist by individuals but also governmental bodies and private corporations, with all the affairs running on the virtual world, rules and guidance are needed to ensure all the parties will not harmed or be harmed by each other.

ICT and Cyber Security in ASEAN

The growth of ICT in Southeast Asia is actually not too far behind the US, Europe and countries in Northeast-Asia like Japan and Republic of Korea. According to ASEAN E-Commerce Database Project released in 2010, ASEAN represent 6 percent of the Internet world users and the sum of global penetration level of ASEAN members countries are 20 percent, with Brunei Darussalam, Singapore and Malaysia having the biggest share of internet penetration, and Indonesia, Philippines, and Vietnam having the greatest numbers of internet user.

Although compared to global number of internet users, 6 percent seems small and insignificant, one cannot forget that ASEAN is holding almost one-tenth (9 percent to be precise) of the world population, far above the population of 28 member countries European Union combined. With this percentage, ASEAN is in a good position to build an advanced ICT region with internet businesses run on it or quoting the report released in the ASEAN E-Commerce Database Project, "...undoubtedly a good environment for the E-Commerce" (ASEAN E-Commerce Database Project, 2010, p. 68).

Moreover, ASEAN has made a considerable progress in ICT development. ASEAN incorporates ICT development as one of the connectivity aspect in its recent master plan on building of ASEAN Community 2015. The Master Plan on ASEAN Connectivity encompasses physical, institutional and people-to-people connectivity with ICT as integral part of physical connectivity. The most recent ASEAN master plan released in 2011 is the ASEAN ICT Master Plan which gives more detailed information on how ASEAN wants to develop its ICT sector.

ASEAN's vision to build the ICT sector is to create a technologically advance and well-connected region. But ASEAN's development on ICT is lacking in incorporating the security aspect. Knowing the important yet fragile system of ICT, ASEAN needs to be ready to face cyber threat that might occur. So far, nine out of ten ASEAN member countries have Computer Emergency Response Team (CERT), the only country remained is Laos who has not establish their CERT. CERTs of the nine countries also are members of Asia Pacific Computer Emergency Response Team (APCERT), a regional organization consist of 29 teams of CERT (21 teams are full member and 8 teams are general member) from 22 Asia Pacific Countries (APCERT, n.d.). The existence of CERT team is vital to be "cyber police" to secure the national cyberspace, and the cooperation among them is needed to build a network to fight cybercrime.

With proper instruments available in most of ASEAN member countries, the question remains whether the instruments are compatible enough to deal with the

reality of cyber threat.

Table 1. ASEAN Internet Penetration

No.	Country	Internet Penetration	Internet Users	Population
	Brunei Darussalam	**81% (1)**	318.900	395.027
	Singapore	**78% (2)**	3.658.400	4.701.069
	Malaysia	**65% (3)**	16.902.600	26.160.256
	Philippines	30%	**(2) 29.700.000**	99.900.177
	Vietnam	27%	**(3) 24.269.083**	89.571.130
	Thailand	26%	17.486.400	66.404.688
	Indonesia	12%	**(1) 30.000.000**	242.968.342
	Lao PDR	8%	527.400	6.993.767
	Cambodia	1,3%	13.800.000	173.675
	Myanmar	0,2%	53.414.374	110.000
ASEAN		20%	604.308.830	123.146.458

(Table from ASEAN E-Commerce Database Project, 2010, p. 14)

Evolution of the New Threats

Before discussing about the evolution of cybercrime, knowing types of that new threat is useful to know. The author will refer to the typology of Council of Europe's Convention of Cyber Crime held in Budapest on 2001. The convention divides four basic types of offences, they are: (1) "Offences against the Confidentiality, integrity, and availability of Computer data and systems" (including illegal access, illegal interception, data interference, system interference, misuse of device), (2) "Computer related offences" (computer related forgery, computer related fraud), (3) "Content related offences" (including child pornography), and (4) "Offences related to infringements of copyright and related rights".

These offences are the formal typology for popular terms like hacking, phishing, spreading *worm, trojan,* malware, or spyware, and illegal downloading.

"A Good Decade for Cybercrime", a report released by McAfee in 2010, covering the growth of trends of cybercrime all over the world shows dynamic changes on cyber-crime that occurred. Ten years turns out to be a sufficient time to see how cybercrime motives are adapting to current situation that time. Divided by four time periods, the years from 2000 to 2010 captured some specific advancements of the use of internet follows by the cybercrime grew along the way. The first period (2000-2003) featured crimes like Distributed Denial of Service (DDoS), Macro viruses, identity theft through unsecured Wi-Fi and harmful MP3 downloads. These kinds of disturbances are still minor compared to what second period caused. The second period (2004-2005) was the time when cybercrime actors tend not only to show off their skill to manipulate digital world but the goal is to make profit from their crime. The spread of adware, spyware, *rootkit*, and *botnets* started to threaten personal users and companies for their capability in stealing important financial information, as

well as damaging their system. The third period (2006-2008) was when the actors started to assemble and act as an organized group. In this period the transnational nature of cyber became increasingly clear, since the group can spread beyond a country border and only connected through cyber space. The last period (2009-2010) captured the recent phenomenal trend of internet product, the Social Network Sites (SNS) that can cause a serious problem through personal information theft, the spread of fraud post or massage, and harmful links (McAfee, 2010, p. 4-6).

In line with the McAfee 2010 report that predicts cybercrime will go mobile in the near future, some other reports also show the cybercrime threat is escalated beyond PC. Norton Cybercrime Report released in 2012 stating this issue, giving the number of two-third adults use mobile gadget to access the internet, and two-third of that amount do not provide their gadget with security tools, the report also wrote that the mobile vulnerability is growing twice as big from 2010 to 2011 (Symantec, 2012).

These reports show that cybercrime threats have escalated in many level, and the complexity rises when it grew strong enough to threat national security. Some cases of cybercrimes are addressed to attack the government institution, and as the trend of cybercrime evolves to a bigger scheme the term "cyber war" becomes popular. However, there is still a debate about the validity to call the "cyber war" as "war". An article by Professor Sean Lawson written in Forbes on 2011 pictured one of the debates between the supporter and the opponent in the issue (Lawson, 2011). Dr. Thomas Rid, who is not agreeing on the term "cyber war", stated his disbelieve clearly from his essay's title "Cyber War Will Not Take Place." The base of his stand point is Clausewitz's theory of war. According to Rid, cyber war doesn't meet the main element of war, that are violent, instrumental, and political (Rid, 2011, p. 10). Meanwhile, Jeffrey Carr, countering this argument in his blog post titled "Clausewitz and Cyber War", assert the approach of using a conventional war theory to analyse cyber war is not suitable since changes happen in the world. In his book written before this debate, "Inside Cyber Warfare" (2010) Carr also explains thoroughly about this trends and the implication to global community.

Despite the debate on the validity of the term cyber war, the effect of cybercrime in small scheme as well as enormous scheme is devastating, caused a major economic lost, even endanger diplomatic relation. A report released by KMPG in 2011, features economic lost in some countries, showing staggering numbers, range from EUR 17 Million (US$ 22 Million) in Germany phishing activity in 2010, US$ 560 million in US information lost calculation in 2009 to GBP 27 billion (US$ 43) from UK annual cost (KPMG, 2011, p. 8).

In the issue of cybercrime is endangering diplomatic relation, cyber war in eastern part of Europe, Middle East conflict which is "going-cyber" or hostility between United States and China that is also spread to cyberspace are the evidences of political motives that might drive the attack.

Two latest notable examples of Eastern Europe cyber war are cyber conflict between Russia-Estonia (2007) and Russia-Georgia (2008). The first case was evoked by Estonian government that moved a memorial of Soviet War from Tallin in 27 April 2007 that provoke Kremlin's rage (The Guardian: Russia accused of unleashing cyber war to disable Estonia, 2007), later the Estonian e-government system and commercial websites included banking system were heavily attacked. According to Estonian Ministry of Defence some of the attacks, although denied by the Russia, are hosted by Russian state servers. (BBC:

Estonia hit by 'Moscow cyber war', 2007). The latter case between Russia and Georgia is a part of two countries conflict concerning the two area South Ossetia and Abkhazia (The Guardian: South Ossetia: Georgia preparing for war, Russia claims, 2008), as well as launched real military attack, Russia also delivered cyber disturbance to several Georgia's state server and commercial websites (The Telegraph: Georgia: Russia 'conducting cyber war', 2008).

In Middle East conflict, one of the case that successfully stole the international headlines was the Stuxnet attack addressed to Iran nuclear facility in 2010, the attack was suspected to be an act from another country (The Guardian: Stuxnet worm is the 'work of a national government agency', 2010).

Last but not least is the US-China cyber warfare. As heat of competitiveness from both countries rises, the cases of cyber-attack coming from the US and China also escalate. The latest news about the attack came from White House, confirming an attack had been launched to their network system (Reuters: White House targeted in cyber-attack, 2012). Although the source was not pointed to China by White House authority, but Freebeacon, a Washington conservative group, report that the hackers was linked to Chinese government (BBC: White House confirms cyber-attack on 'unclassified' system, 2012).

The cases above shows that cyber-crime trends are going global and the intensity of the attack are increased with lost calculation that not only threatens economically but also politically. Considering the risk, if a region, in this case Southeast Asia, wants to connect its member ICT infrastructures, a security plan must be built to avoid future cybercrime threat.

Countries in Southeast Asia themselves are not save from cybercrime threat. As told above, with the cyber development in this region, the threat of cybercrime is parallel with the advancement. Although most of the problems in Southeast Asia countries that related to internet are concerning on the issue of internet freedom that does not mean there is no threat of cybercrime in the region. Recent *Internet Security Threat Report* released by Symantec shows that Indonesia ranked in 10th place on cyber-crime source, delivering 2,4 percent cyber treat globally (Kompas: Indonesia Masuk 10 Besar Penyumbang "Cyber Crime" Terbanyak, 2012). Another report by Trend Micro Incorporated also picturing the future of cybercrime threat in the region of Asia Pacific (Okezone: Penjahat Cyber Ancam Keamanan di Asia Pasifik, 2012), the report stated that Vietnam rank in the 3rd of source of spam in the region (Networks Asia: Asia-Pacific security landscape shows a mix of old and new threats, 2012).

Cyber Security Cooperation Models

As Cyber Security become a global problem, the need to arrange a cooperation to overcome cybercrime threat is inevitable. Many countries started to realize the importance of having cooperation to tackle the growth of cybercrime. This argument also implied in a statement by Eun-Ju Kim, the ITU (International Communication Union) Regional Director for Asia and the Pacific, "The best way to counter this crime is through close partnerships and cooperation in an interdependent information society" (UNODC, Cybercrime in Asia and the Pacific: Countering a Twenty-First-Century Security Threat)

Dr. Hamadoun Touré in his ITU Publication "Quest for Cyber Peace" (2011) enlists some cooperation addressed to this issue. Some of them are Council of Europe with Convention on Cybercrime 2001, North Atlantic Treaty Organization (NATO)

with Cyber Defence Management Authority, and United Nation which implement cybercrime prevention on some of its branch like the UN Economic and Social Council and United Nations Office on Drugs and Crime.

From all written above, Council of Europe's Convention on Cybercrime (2001) is the earliest international formal cooperation who set the definition, typology, and measures to be taken to cope with cyber-crime. It has signed by 49 countries, four are from outside the Europe, and they are Japan, South Africa, Canada and United States. The numbers who have ratified is 39 countries, as the Belgium as the newest one, who ratified it in 2012, and two countries in latest accession status, Australia in 2012 and Dominican in 2013 Republic (Council of Europe Treaty Office, 2013).

This comprehensively written agreement can be a good source to look at what ASEAN needs to prepare and socialize among each member before working on the actual framework of cyber security cooperation. The most important part to be examine for the future framework is Chapter III of the convention which includes article on extradition (article 24), vast scope of mutual assistance in cyber space (Article 25-35) and active communication (article 35). Regulation regarding extradition is important in cybercrime is a transnational-based crime whose offender can launch their attack from anywhere outside the country. For the later matters on mutual assistance and active communication, these arrangements can answer the fulfilment of gaps between ASEAN countries that more advance parties have the obligation to encourage the region to stand on the same standard before enforcing the cooperation framework.

Another example of cyber security cooperation is offered by NATO with their cyber defence framework. In their document released in 2011, the alliance draft their cyber defence agendas not only in regard of securing the region in defensive mode trough NATO Cyber Defence Management Board and NATO Computer Incident Response Capability, but also integrating it into the national policy of the Alliance members and encouraging education in cyber defence sector with NATO Cooperative Cyber Defence Centre of Excellence (NATO 2011).

NATO's cooperation might seem very organized and can be strongly recommended for ASEAN to build such cooperation, but it has to be realized that NATO and ASEAN have a different platform of cooperation. ASEAN is not security alliance and in ASEAN, where non-interference and sovereignty are two of some basic principles, defence policy is a very crucial aspect to be interrupted. Each country has their own view and ASEAN cannot dictate members' domestic area. The framework of ASEAN future cooperation has to be emphasized on security of the region as a whole without disturbing its member sovereign.

Another example of cooperation, Asia Pacific Computer Emergency Response Team (APCERT), took the form of regional cooperation. APCERT members are CERT and Computer Security and Incident Response Team (CSIRT) of each country, the main legal body in combating cybercrime. Its missions are enhancing cooperation, developing measures to overcome cases, facilitating in information sharing, promoting research and development, assisting conduct on CERT, and providing recommendation on legal issues (APCERT: Missions Statement). Moreover since the members are team of experts, APCERT will be able to focus on the technicalities to overcome cyber threat, event like drill exercise is the one of the main program held annually (APCERT: Operational Framework, p 8).

This model might be the one ASEAN is aiming for, since almost all ASEAN member countries are also joining APCERT it is probably easier to use APCERT model and configure ASEAN's cyber security framework based on that model. However, APCERT is less legitimate than the other two previous examples. As mentioned, APCERT members are only technical bodies of the member states that lacking of political power to make significant policy change. If ASEAN take APCERT format cooperation as a whole, it will only make a cooperation that will overlap with APCERT agenda and will not be powerful enough to make any changes in governmental level.

ASEAN Cyber Security Cooperation in the Future

The first purpose of ASEAN as written in ASEAN Charter "To maintain and enhance peace, security and stability and further strengthen peace-oriented values in the region" (ASEAN Charter, p. 3) was actually the basic duty of ASEAN. This point imply that ASEAN is actually a security community which establishment driven by political motive (Luhulima et al, 2008, p. 71). ASEAN must be prepared for any security threats that challenge the region as the security issues evolve from time to time. But with conventional security conflict like border dispute is still on the headline, ASEAN readiness to enter contemporary security issue is questionable. Yet, ASEAN has planned blueprints and master plans for the realization of ASEAN Community to ensure its path in the beyond 2015 will embrace the needs of future generation. In the case of cyber security, unfortunately the designed documents that supposed to be related to issue like ASEAN Political Security Blueprint, Master Plan on ASEAN Connectivity and ASEAN ICT Master Plan 2015 have not point out significance idea on how ASEAN cyber security will be defined and maintained.

In former documents of ASEAN Regional Forum (ARF), ASEAN has noted the significance of cyberspace issue. It can be found in ARF discussion since 2004 when ARF Seminar on Cyber Terrorism held in South Korea. But not until the meeting in 2006 13th ARF Meeting, it released the Statement on Cooperation in Fighting Cyber Attack and Terrorist Misuse of Cyber Space. Although the statement is not as comprehensive as the Council of Europe's Convention on Cybercrime, the statement already sent a strong message about the agreement among ARF's member states to combat the terrorism including types of terrorism using cyber space as its way for committing their act.

ARF also realize the enormous threat of the cybercrime or cyber misuse as stated below,

> "...terrorist misuse of cyber space is a destructive and devastating form and manifestation of global terrorism whose magnitude and rapid spread would be exacerbated by the increasing cyber interconnectivity of countries in the region;
>
> Recognizing the serious ramifications of an attack via cyber space to critical infrastructure on the security of the people and on the economic and physical well-being of countries in the region" (ARF, the Statement on Cooperation in Fighting Cyber Attack and Terrorist Misuse of Cyber Space, 2006)

But combining cybercrime with

terrorism can cause confusion since both have different context.

Meanwhile many types of cyber misuse, from the small scale of cybercrime to cyber war, are not necessarily related to the act of terrorism. Cyber fraud, phishing, piracy can be driven some other motives that are purely a crime act and not done by a terrorist group who is usually driven by political motive. By this reasoning, defining cybercrime apart from cyber terrorism is important to build basic understanding for cooperation on cyber security.

ASEAN is yet to have a formal agreement on cyber security beyond the ARF statement in 2006. Although the needs of having agreement on cyber security in ASEAN is important, agreeing on an understanding about security in this region is never an easy task. The problem of digital divide or networking advancement gap, among countries of ASEAN is causing different level of concern in each country. For example for an ICT-advanced country like Malaysia, the need of cyber security might be critical to be fulfilled. In his remarks for The Shangri-La Dialogue 2012, Malaysia's Minister of Defence, Dato' Seri Dr. Ahmad ZahidHamidi stated the urgency of to build a more comprehensive cyber-defence as the cyber-attack is increasing (IISS: Fourth Plenary Session). In the other hand, for countries with low number of internet users and internet penetration also not advanced in ICT infrastructure building such cooperation and agreement might not become their priority.

If ASEAN is serious about realizing cyber security cooperation, ASEAN has to know what kind of cooperation that would meet the need of the region. It has been discussed in previous section about three examples ASEAN might want to consider. All formats can give beneficial input for making the framework of future cyber security cooperation; however ASEAN must make some adjustment so the framework will be acceptable to the members of ASEAN. There are three points worth to be taken from those formats. Firstly, ASEAN must stand on the same basic understanding on defining and treating the issue of cyber security and cyber threats. Secondly, ASEAN member countries must willing to put the issue of cyber security as of their priority area, by doing so, the policy made in the regional level will be easier to implement in national level. Thirdly, cooperation in technical level must be taken seriously because networking security will need to run smoothly if every party have the same technical capability.

For the format of cooperation, APCERT actually is a good base for further development of stronger ASEAN cyber cooperation in the future. But with the objective to secure ASEAN's ICT network planned in the Master Plan on ASEAN Connectivity and ASEAN ICT Master Plan, cooperation framework like APCERT must be strengthen. One of the ways for strengthening the format of APCERT is by raising the cooperation into higher level, such approach will deliver stronger political power so it will have significant authority to push its agenda in national government level. A binding document like Council of Europe's Convention of Cybercrime also can inspire ASEAN's cyber security cooperation framework, however basic understanding on the issue must be form in advance. The future cooperation also has to be designed carefully that it will respect ASEAN's principles of non-inference and sovereignty.

Conclusion

Picturing ASEAN to be a connected region in ICT infrastructure is a great vision it might need for realizing its goal in economic and socio-culture pillars. The

vision, as stated in ASEAN ICT Master Plan 2015 is heading "Towards an Empowering and Transformational ICT: Creating an Inclusive, Vibrant and Integrated ASEAN" (ASEAN, ASEAN ICT Master Plan 2015, p. 12). But this vision came with complex arrangement to be prepared. The first one is to equalize the infrastructure, knowledge and competence on ICT in ASEAN member countries, and the second one is to prepare the safety procedure for running a connected region that lies on ICT.

The establishment of ASEAN ICT connectivity might be addressed for economic and social development of the region and placed below the pillar of economic with ASEAN Telecommunications and IT Ministers Meeting (TELMIN) as the one in charge for drafting master plan, but this arrangement will be prone to security implication if it does not have a proper protection from cybercrime threats. For this reason, the agreement on how ASEAN will secure its future ICT connectivity is required.

Since most countries in ASEAN already have their CERT team, that can be imply the countries have realized the significance of securing their cyberspace. Cooperation among those teams is also necessary because cybercrime is a contemporary threat to security which runs on a borderless cyberspace. But to enhance the level of cooperation, a more powerful form of formal agreement have to be conducted so ASEAN member countries will have the same interpretation on defining cybercrime and ensuring their steps on overcoming the problem is orginized in the suitable framework. The agreement also have to cover the borderless nature of cybercrime, enables ASEAN member countries to investigate cybercrime case in neighbouring countries in the region and processed the case according to regional agreement.

Building that agreement might not be an easy task, since cyber security is not yet considered as a priority and issues like state border disputes are considered to be more critical to solve. Moreover, putting cyber security as an issue for convention like the Council of Europe did in Budapest will require ASEAN member states to adjust their national law once they ratified the convention. This adjustment usually initiates domestic debate for its relation to sensitive issues of national security and sovereignty. Hence configuring an acceptable draft for this agreement is necessary to make sure ASEAN member countries are willing to sign and ratify it.

*****

About Author

Khanisa, SIP – Graduated from Bachelor degree in International Relations Department of Faculty of Social and Political Science, Gadjah Mada University in 2010, she is currently taking Master degree in Graduate Studies in International Affairs at College of Asia and The Pacific, Australian National University. Her work as a researcher started in 2011 as junior researcher in Centre for Political Studies (Pusat Penelitian Politik-P2P) at Indonesian Institute of Sciences (Lembaga Ilmu Pengetahuan Indonesia). Her research interests are the significance of and Information and Communications Technology (ICT) and social media in international relations and issues regarding the region of Southeast Asia and ASEAN.

Acknowledgement

The author would like to express her gratitude to Dr C. P. F. Luhulima for his input and suggestions in writing this paper.

Notes

This paper was presented on 7 November 2012 at The First International Conference on Business, International Relations, and Diplomacy 2012, in Binus University Jakarta with the same title, later revision is added to meet current situation and updates.

References

ASEAN Regional Forum 28 July 2006, *Statement on Cooperation in Fighting Cyber Attack and Terrorist Misuse of Cyber Space,* ARF Chairman's Statements and Report, viewed 27 July 2013, <http://aseanregionalforum.asean.org/files/library/ARF%20Chairman%27s%20Statements%20and%20Reports/The%20Thirteenth%20ASEAN%20Regional%20Forum,%202005-2006/ARF%20Statement%20on%20Cooperation%20in%20Fighting%20Cyber%20Attack%20and%20Terrorist%20Misuse%20of%20Cybe%20Space%20(Final).doc>

ASEAN Telecommunications and ICT Senior Officials' Meeting 10 November 2010, *The ASEAN E-Commerce Database Project* (Ref No. DTI/ASEANTELSOM/01), ASEAN, viewed 27 July 2013, <http://www.asean.org/images/2012/publications/ASEAN%20eCommerce%20Database%20Project.pdf>

Asia Pasific Computer Emergency Response Team 2010, *Asia-Pasific Computer Emergency Response Team (APCERT) Operational Framework*, Asia Pasific Computer Emergency Response Team, viewed 27 July 2013, <http://www.apcert.org/documents/pdf/OPFW_3March10.pdf>

Asia Pasific Computer Emergency response Team, *Member Teams,* Asia Pasific Computer Emergency Response Team, viewed 27 July 2013, <http://www.apcert.org/about/structure/members.html>

Asia Pasific Computer Emergency response Team, *Mission Statement,* Asia Pasific Computer Emergency Response Team, viewed 27 July 2013, <http://www.apcert.org/about/mission/index.html>

Association of Southeast Asian Nations 2007, *The ASEAN Charter*, Association of Southeast Asian Nations, viewed 27 July 2013, <http://www.aseansec.org/wp-content/uploads/2013/06/ASEAN-Charter-1.pdf>

Association of Southeast Asian Nations 2011, *Master Plan on ASEAN Connectivity* , Association of Southeast Asian Nations, viewed 27 July 2013, <http://www.aseansec.org/wp-content/uploads/2013/06/ASEAN-Charter-1.pdf>

British Broadcasting Corporation 2007, *Estonia hit by 'Moscow cyber war'*, BBC News online (Last updated: 15:21 GMT 17 May 2007), viewed 27 July 2013, available at <http://news.bbc.co.uk/2/hi/europe/6665145.stm>

British Broadcasting Corporation 2012, *White House confirms cyber-attack on 'unclassified' system*, BBC News online (Last updated: 20:21 GMT 1 October 2012), viewed 27 July 2013, available at <http://www.bbc.co.uk/news/world-us-canada-19794745>

Carr, J 2010, *Inside Cyber Warfare*, O' Reily Media Inc , Sebastopol, CA.

Carr, J. 2011, 'Clausewitz and Cyber War', weblog post, October 23, viewed 1 October 2012, <http://jeffreycarr.blogspot.com/2011/10/clausewitz-and-cyber-war.html>

Chadbourn, M. 2012, *White House targeted in cyber attack,* Reuters News online, (Last Updated: 3:28pm EDT 1 October 2012), viewed 27 July 2013, available at <http://www.reuters.com/article/2012/10/01/

net-us-usa-whitehouse-cybersecurity-idUSBRE89016O20121001>

Council of Europe 2001, *Convention on Cybercrime*, Council of Europe, viewed 26 July 2013, <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>

Council of Europe Treaty Office 2013, Council of Europe, Budapest, viewed 26 July 2013 <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG>

Gercke, M 2011, *Understanding Cybercrime: A Guide for Developing Countries.*

Halliday, J. 2010, *Stuxnet worm is the 'work of a national government agency'*, The Guardian online, (Last Update: 00.35 AEST 25 September 2010), viewed 27 July 2013, available at <http://www.guardian.co.uk/technology/2010/sep/24/stuxnet-worm-national-agency>

International Telecommunication Union, Cybercrime Legislation Resources, Geneva, Switzerland: International Telecomunication Union, viewed 27 July 2013, <http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITU_Guide_A5_12072011.pdf>

KPMG International 2011, *Cyber Crime - A Growing Challenge for Governments. Issues Monitor, vol. 8, July*, KPMG International, viewed 27 July 2013, <http://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/Documents/cyber-crime.pdf>

Lawson, S. 2011, *Cyber War and the Expanding Definition of War, sites*, October 26. Forbes, viewed 27 July 2013, <http://www.forbes.com/sites/seanlawson/2011/10/26/cyber-war-and-the-expanding-definition-of-war/>

Luhulima, CPF, et al, 2008, *Masyarakat Asia Tenggara MenujuKomunitas ASEAN 2015*, Yogyakarta and Jakarta, PustakaPelajar and P2P-LIPI, Indonesia.

Luthfi, A 2012. *Penjahat Cyber AncamKeamanan di Asia Pasifik*, Okezone online, (Last Update: 12:03 GMT+7 15 Agustus 2012), viewed 27 July 2013, available at: <http://techno.okezone.com/read/2012/08/15/55/677948/penjahat-cyber-ancam-keamanan-di-asia-pasifik>

NATO 2011, Defending the Networks: The NATO Policy on Cyber Defence, NATO, Belgium, viewed 26 July 2013 <http://www.nato.int/nato_static/assets/pdf/pdf_2011_09/20111004_110914-policy-cyberdefence.pdf>.

Networks Asia. 2012. *Asia-Pacific security landscape shows a mix of old and new threats, Networks Asia online, (Last Update: 25* July 2012), viewed 27 July 2013, available at: <http://www.networksasia.net/content/asia-pacific-security-landscape-shows-mix-old-and-new-threats>

Norton by Symantec 2012, *2012 Norton Cybercrime Report*, Norton, viewed 27 July 2013, <http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf>

Panji, A. 2012, *Indonesia Masuk 10 Besar Penyumbang "Cyber Crime" Terbanyak*, Kompas online. (Last Update: 09:40 GMT+7 16 May 2012), viewed 27 July 2013, available at: <http://tekno.kompas.com/read/2012/05/16/09403718/Indonesia.Masuk.10.Besar.Penyumbang.Cyber.Crime.Terbanyak>

Rid, T 2012,'Cyber War Will Not Take Place',*Journal of Strategic Studies*, vol 35, no 1, 5-32.

Ryan, J 2010, *A History of The Internet and Digital Future,* Reaktion Books, London, UK.

Singh, P Kr 2007, *Laws on Cyber Crimes Alongwith IT Act and Relevant Rules*, Book Enclave, Jaipur, India.

Swaine, J 2008, *Georgia: Russia 'conducting cyber war'*. The Telegraph online. (Last Update: 11:11AM BST 11 Aug 2008), viewed 27 July 2013, available at:<http://www.telegraph.co.uk/news/worldnews/europe/georgia/2539157/Georgia-Russia-conducting-cyber-war.html>

The 10th ASEAN TELMIN 2011, *ASEAN ICT Masterplan 2015*, ASEAN, viewed 27 July 2013, <http://www.asean.org/images/2012/publications/ASEAN%20ICT%20Masterplan%20%28AIM2015%29.pdf>

The International Institute for Strategic Studies - Dato' Seri Dr. Ahmad ZahidHamidi 3 June 2012, *Remarks on The International Institute for Strategic Studies, The Shangri-la Dialogue 2012*, The International Institute for Strategic Studies, viewed 27 July 2013, <http://www.iiss.org/conferences/the-shangri-la-dialogue/shangri-la-dialogue-2012/speeches/fourth-plenary-session/ahmad-zahid-hamidi/>

Touré, HI 2011, *The Quest For Cyber Peace*, International Telecommunication Union and World Federation of Scientists, Geneva, Switzerland, viewed 27 July 2013, <http://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-WFS.01-1-2011-PDF-E.pdf>

Traynor, I 2007, *Russia accused of unleashing cyberwar to disable Estonia,* The Guardian online, (Last Update: 17 May 2007), viewed 27 July 2013, available at: <http://www.guardian.co.uk/world/2007/may/17/topstories3.russia>

United Nations Office on Drugs and Crime 20 October 2011, *Cybercrime in Asia and the Pacific: countering a twenty-first-century security threat.* United Nations, viewed 27 July 2013, <http://www.unodc.org/unodc/en/frontpage/2011/October/cybercrime-in-asia-pacific_-countering-a-21st-century-security-threat.html>

Womack, H 2008, *South Ossetia: Georgia preparing for war, Russia claims,* The Guardian online, (Last Update: 8 August 2008), viewed 27 July 2013, available at : <http://www.guardian.co.uk/world/2008/aug/08/georgia.russia>